PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
System Design & Engineering

Fee Basis Claims System (FBCS) Bridge Contract

Date: April 11, 2016
TAC- FY-17-32040
PWS Version Number: 0.1

Contents

1.0 BACKGROUND

Department of Veterans Affairs (VA), Veteran's Health Administration (VHA) is one of the world's largest health care delivery organizations. As part of an integrated strategy to provide Veterans with timely access to quality health care services, VA healthcare facilities are authorized to pay for health care services acquired from non-VA health care providers. These services may be provided to eligible Veterans from non-VA health care providers when VA determines medically necessary services are not available from VA on a timely basis, in an emergency, or when VA or other Federal facilities are not feasibly available.

VA manages the authorization, claims processing and reimbursement for services acquired from non-VA health care providers through the Purchased Care Program. The basic provisions of and authority for the Purchased Care Program are provided through public laws passed by Congress. These laws have been codified into the United States Code (38 USC 1703, 1725 and 1728) and further clarified in various Code of Federal Regulations.

FBCS allows Fee Claims processing departments to manage and process Fee claims in an electronic environment which improves the ability to keep track of claims in-process and enables identification of duplicate and non-compliant claims. In addition, FBCS improves VA's ability to report on Fee expenditures and improves accuracy and consistency of Fee authorizations. FBCS provides the ability to monitor individual and department productivity. In addition, FBCS allows VA to communicate efficiently with the vendors and Veterans about the adjudication status of their claims by providing a complete audit trail for each claim.

OI&T intends to transition projects from the PMAS project management process into the Veteran-focused Integration Process (VIP) project management process in the 2016-2017 timeframe (https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371). The Veteran-focused Integration Process (VIP) is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise.

VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence.

VIP is a significant evolution from PMAS, creating a more flexible process that has fewer documentation requirements and milestones, and delivers products in shorter

increments. VIP is currently undergoing a Pilot Program and is currently in a draft state and will continue to evolve. Once the pilot is complete, requirements outlined in this PWS may be transitioned to the VIP framework during the Period of Performance of this contract.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www.va.gov/vapubs
10. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
11. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
13. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
18. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
19. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
20. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012

21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
25. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
26. OI&T ProPath Process Methodology (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp
    NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
27. One-VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
28. National Institute Standards and Technology (NIST) Special Publications (SP)
29. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, “Transition to IPv6”, September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
37. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013

43. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
44. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
46. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
50. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
52. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
56. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
57. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
58. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
59. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
60. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
61. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
62. VA Directive 6071, Project Management Accountability System (PMAS), February 20, 2013

63. VA Memorandum, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems”, (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
64. VA Memorandum “Mandatory Use of PIV Multifactor Authentication to VA Information System” (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
65. VA Memorandum “Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges” (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

3.0 SCOPE OF WORK

The scope of this procurement includes the renewal of 142 software licenses, maintenance and technical support for the Fee Basis Claims System (FBCS) at the 142 end user sites where FBCS is currently deployed as listed in Attachment A. The Contractor shall provide annual software licenses, and software maintenance services, which include periodic updates, upgrades, enhancements and corrections to the software, training, and technical support, so as to cause the software to perform according to its specifications, documentation or demonstrated claims. The scope includes modification of the FBCS product to meet regulatory and legislative requirements so that the Government may properly pay claims.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be from October 1, 2016 through September 30, 2017, followed by four 6-month option periods and one 3-month option period.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at the Contractor's facilities.

4.3 TRAVEL

The Government anticipates travel under this contract to perform the tasks associated with the FBCS effort, as well as to attend program-related meetings or conferences through the period of performance. Include all estimated travel costs in your firm-fixed price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program related meetings for this effort is four trips to Denver, Colorado per year for four travelers for three days per trip.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated monthly thereafter. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor shall keep in communication with the VA to ensure that issues that arise are transparent to both parties and are being addressed in a timely manner.

The Contractor shall provide a Production and Operation Manual (POM) for the infrastructure and software solution (in accordance to ProPath template at http://vaww.oed.wss.va.gov/process/Library/Forms/Default.aspx). The manual shall be sufficient to support ongoing operations by trained VA personnel, system administrator and Contractors/SMEs providing sustainment with responsibility clearly shown in an O&M responsibility matrix. The POM shall be written in a manner in which the VA site personnel can startup, configure, operate, shutdown, and apply firmware and software

upgrades to individual devices and applications without the need for technical support from the Contractor. The POM shall be written to allow the VA site personnel to troubleshoot, repair, or replace equipment down to the box level consistent with the original equipment manufacturer specifications. The POM shall include a table delineating Responsible/Accountable/Consulted/Informed (RACI) assignments for system functionality.

The Contractor shall deliver updated FBCS application and system architecture diagrams reflecting the VA installation with any updates as required.

Deliverables:

A. Contractor Project Management Plan
B. Production and Operations Manual (POM)
C. Updated FBCS Application and System Architecture Diagrams

5.1.2 KICKOFF MEETING

The Contractor shall conduct a project kickoff meeting no more than ten business days after contract award to introduce the Government team to the Contractor's overall operating plans and approach to this work. The Contractor shall present and be prepared to discuss the content of the CPMP. The Contractor shall deliver kickoff meeting minutes no later than one week after the meeting and shall identify all the discussion points, agreements and action items. The Contractor shall present the CPMP including staffing, quality and risk plans, overall work plans, and integrated schedules for this project. The Contractor shall present known risk areas and shall review its detailed POM.

Deliverables:

A. Kickoff meeting minutes

5.1.3 REPORTING REQUIREMENTS

The Contractor's project manager and appropriate technical staff shall attend weekly status meetings with the VA Project Manager (PM) to discuss the progress of all contract-related activities. The Contractor shall provide a bi-weekly (every other week) report reflecting products delivered, deliverables in progress, known exceptions to performance standards, as well as any issues or risks relevant to the FBCS Program. The VA Contracting Officer's Representative (COR) may require more frequent meetings or reports as needed.

The Contractor shall provide timely responses to questions, written requests and inquiries regarding technical aspects of project management artifacts within five workdays of the initial request.

Deliverable:

A. Bi-Weekly Progress Reports

5.2 SOFTWARE LICENSE, MAINTENANCE AND SUPPORT REQUIREMENTS

The Contractor shall provide renewal of 142 FBCS licenses identified in Attachment A, maintenance, and support of Purchased Care claims management and adjudication. FBCS software includes the following functionality:

A. Referral Management
B. Claims Processing
C. Document Management
D. Appeals Management
E. Financial Management
F. Correspondence
G. Revenue Management
H. Reporting
I. Interfaces
J. User Management
K. Work Management

Definitions:

A. Licensee. The term “licensee” shall mean the U.S. Department of Veterans Affairs (“VA”) and is synonymous with “Government.”
B. Licensor. The term “licensor” shall mean the software manufacturer of the computer software being acquired. The term “Contractor” is the company identified in Block 17a on the SF1449.
C. Software. The term “software” shall mean the licensed computer software product(s) cited in the Schedule of Supplies / Services. (SF1449, Block 20).
D. Release or Update. The term “release” or “update” are terms that refer to a revision of software that contains defect corrections, minor enhancements or improvements of the software’s functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.
E. Version or Upgrade. The term “version” or “upgrade” are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

5.2.1 LICENSE AND GRANT OF LICENSE

A. The Contractor shall deliver the annual FBCS site licenses and software renewal to VA in accordance with the Schedule. The software license provided to the Government under this Contract is an irrevocable, nonexclusive license to use the software.

B. If the licensed software requires a password (or license key) to be operational, it shall be delivered with the software media and have no expiration date.

C. If the Government decides to outsource or contract its services, the Government may allow the outsourcer to use the licensed software solely to provide the services on its behalf. The outsourcer shall be bound by the provisions of this Contract relating to the use of the software.

D. VA may use the software in a networked environment.

E. Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).

F. If for any reason the Contractor is unable to complete performance under this Contract or, if following the completion of this Contract, the Contractor ceases to provide support for any software described in this Contract, the Contractor agrees to provide to Government any proprietary software or documentation that is relevant to the work performed under this Contract. This provision applies to any data that would be necessary for the maintenance and continued development of any automated information systems, including at a minimum: system source and object codes, supporting system software and all relevant documentation and source listings. This data shall be provided to the Government at no additional cost within thirty (30) calendar days following work stoppage.

G. VA has the right to move and use the software to any VA location at no additional licensing cost.

H. The Contractor shall deliver all source code and data developed by Contractor under this Contract to VA upon request at no additional cost to the Government.

I. All limitations of software usage are expressly stated in the SF 1449 Sections A, B, C & D.

J. The Contractor shall deliver FBCS technical documentation in electronic format to include:

   1. system configuration documentation
   2. technical manuals
   3. installation guides

K. All software licensed under this contract is Proprietary Restricted computer software. It was developed at private expense and is copyrighted, including minor modifications of the computer software, all rights reserved, and is licensed only for use in connection with this contract. However, VA shall have unlimited rights in any and all data first produced at Government expense by DSS under this Contract or any previous contract or order in accordance with FAR 52.227-14.

Deliverables:

A. FBCS site licenses
B. FBCS technical documentation

5.2.2 FBCS SOFTWARE MAINTENANCE AND TECHNICAL SUPPORT

The Contractor shall provide software maintenance and technical support services, which include periodic updates, enhancements and corrections to the software. Maintenance and support includes software bug fixes; telephone and e-mail support of the FBCS product; and interfaces, both non-VistA interfaces and those supported by VA Interface Control Registrations (ICRs). See list in Attachment B. VA will notify the Contractor as soon as changes affecting an interface are approved. The Contractor shall coordinate with the COR any changes to their software that might impact VA systems.

The Contractor shall provide computer software that does not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable the software. Such code includes at a minimum a computer virus, restrictive key, node lock, time-out or other function, whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration or use, or other limiting criteria. If any such code is present, the Contractor shall indemnify the Government for all damages suffered as a result of a disabling caused by such code, and the Contractor shall remove such code upon the Government's request at no extra cost to the Government. Inability of the Contractor to remove the disabling software code shall be considered an inexcusable delay and a material breach of the Contract, and the Government may exercise its right to terminate for cause. In addition, the Government is permitted to remove the code as it deems appropriate and charge the Contractor for consideration for the time and effort in removing the code.

5.3 HELP DESK SUPPORT

The Contractor shall provide help desk support to the FBCS application. The Contractor shall operate a help desk and provide help desk staffing located in Contractor facilities. The Contractor shall provide:

1. Support for all hours of operation (8:00 a.m. to 7:30 p.m. Eastern Standard Time (EST), Monday through Friday (excluding Federal Holidays) and after hours emergency coverage as required.
2. On-call support for emergencies such as application unavailability due to software bugs, software patches, and software updates.

The Contractor shall provide application support to resolve FBCS user questions, issues, and problems. Documentation supporting all issues shall be maintained in the Help Desk ticket tracking tool (VA's incident management systems).

The Help Desk shall provide notification to the COR of issues impacting more than one site or impacting any single site for longer than one business day.

The Contractor shall use VA's incident management systems for reporting of trouble tickets by VA users. The Contractor shall document problem resolution so that the VA solutions database can be updated. The Contractor shall provide:

A. Email Support:
    1. The Contractor shall provide a Help Desk email mailbox for reporting problems by electronic mail.
    2. The Contractor shall monitor the FBCS Help Desk email account and respond via email or telephone, as appropriate, based on the priority of the ticket.
    3. For all tickets, the Contractor shall send the user an automated email notification of the ticket number and priority.

B. Telephone Support
    1. Calls shall be answered within 30 seconds.
    2. For all tickets, the Contractor shall send an e-mail to the user notifying the user of the ticket number and priority.
    3. The Help Desk shall generate or update a ticket for each call incident.
    4. Callers shall have the option to leave a voice mail. Voice mail messages received during duty hours must be responded to within 30 minutes.
    5. Voice mail messages received after duty hours shall be answered by 8:30 AM EST the next work day.

C. Ticket Priorities
    1. Critical (Emergency) Priority – user is experiencing fatal system error, loss of data or a system outage is occurring impacting multiple sites. Immediate within 2 hours, notification to the COR is required for any critical priority.
    2. High Priority – system issue causing improper payment. High priority tickets require notification to the COR within one business day
    3. Medium Priority – user is experiencing inability to perform specific functionality but not experiencing fatal error or loss of data.
    4. Low Priority – user has normal inquiries for changes in configuration or questions on how to perform specific system functions.

D. Resolution Time to Ticket Priorities
    1. Critical (Emergency) Priority Resolution –The request shall be resolved within 2 hours. If the issue has not been resolved after 2 hours, then the Contractor shall provide hourly progress reporting to VA.

The Contractor shall provide a Bi-weekly Help Desk Activity Report to the COR with a copy to the VA PM. The report shall be submitted via email and is due with the Bi-Weekly Progress Reports. Highlights of this report will be discussed at the weekly status meeting. This report shall contain the following information for both telephone and email support:

A. Period covered by report
B. Call volume statistics
C. Statistics on average wait times for initial responses
D. Documentation of unresolved requests
E. Documentation of Frequently Asked Questions
F. Lessons learned

The Contractor shall create an incident ticket for any issue that is not immediately resolved. The Contractor shall provide a Bi-weekly Incident Ticket Report containing a synopsis of all tickets open longer than 30 days. The report shall be submitted via email and is due with the Bi-Weekly Progress Reports. Highlights of this report will be discussed at the weekly status meeting. This report shall contain the following information:

A. Period covered by report
B. Ticket priority (Critical, High, Medium, Low)
C. Date received
D. Facility
E. Ticket number
F. Summary of issue
G. Current status
H. Anticipated resolution date

Deliverables:

A. Bi-weekly Help Desk Activity Report
B. Bi-weekly Incident Ticket Report

5.4 TRAINING AND DOCUMENTATION

5.4.1 TRAINING

The Contractor shall provide training within 30 days of implementation of new releases when enhanced functionality is introduced; this training may be provided via distance learning and shall be coordinated with the COR.

5.4.2 TRAINING DOCUMENTATION

All user documentation listed below shall be delivered to VA within 30 days of implementation of any modifications to the software and shall be provided in electronic format (either Word or pdf).
Training materials shall include:

A. student and trainer guides
B. user manuals
C. quick reference sheets.

Deliverable:

A. Updated Training Materials

5.5 TESTING AND RELEASE

The Contractor shall follow OI&T testing and release processes for FBCS. Any alternate testing processes must be approved in writing by the COR prior to implementation. The Contractor shall perform regression testing as operating systems or hardware is upgraded. As aging hardware is refreshed, the Contractor shall install and/or regression test the FBCS application.

Deliverables shall include an updated master test plan for interfaces and a test analysis results report.

Deliverables:

A. Updated Master Test Plan
B. Test Analysis Results Report

5.6 ALASKA FEE SCHEDULE

Non-VA providers are paid utilizing the Alaska Fee Schedule in accordance with 38 CFR 17.56, VA payment for inpatient and outpatient health care professional services at non-departmental facilities and other medical charges associated with non-VA outpatient care (b), specifically addresses the special circumstances for physician and non-physician professional services rendered in Alaska.

The Contractor shall update the FBCS software each January to apply the following business rules to automatically calculate payment for claims as required for the state of Alaska:

a. Use previous year's Alaska Fee Schedule and allowable rates will be used to update the schedule for the following year.
b. For services represented by Healthcare Common Procedure Coding System (HCPCS) level I and II codes established after December 31, 2015, apply the Centers for Medicare & Medicaid Services (CMS) rate for each code with

a newly established CMS rate or; Apply a new code and multiply it times the average percentage paid by VA in Alaska for CMS-like codes to establish a baseline amount for these codes.

c. Update the rates in accordance with VA and the Medicare Economic Index annual inflation rate adjustments.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating

system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program,")
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☒	☐	☐
5.2	☐	☒	☐
5.3	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐
5.6	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints

f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	**Performance Standard**	**Acceptable Performance Levels**
A. Technical Needs	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in timely manner 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality	Satisfactory or higher

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) using either POE or GFE or RESCUE with GFE are the current and only VA approved methods for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-

provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media). All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government will supply laptops for Contractor access to VA systems for FBCS maintenance and troubleshooting. Laptops shall be returned to VA at the conclusion of the contract, or whenever they are no longer required for system access, whichever occurs first.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications

- ☐ § 1194.23 Telecommunications products
- ☐ § 1194.24 Video and multimedia products
- ☐ § 1194.25 Self contained, closed products
- ☐ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.4. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any

request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.

3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified

product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the

Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program and theTIC Reference Architecture*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *VA Privacy Impact Assessment*.

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”),

throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation.

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are

to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization) (C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems

must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification,

VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per

affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

POINTS OF CONTACT

VA Program Manager:
Name: Richard Holmes
Voice: 801 605-8413
Email: Richard.Holmes@va.gov

Contracting Officer's Representative:
Name: Robert Rupe
Address: 7185 Bright Ave
Cocoa, FL 32927
Voice: 321 322-7943
Email: Robert.Rupe@va.gov

ATTACHMENT A: FEE BASIS CLAIMS SYSTEM END USER SITES

Line item	VISN	STATION	STATION NAME	CITY	STATE	SITE TYPE
1	1	402	VA Maine Health Care Systems (Togus)	Augusta	ME	Large
2	1	405	White River Junction VAMC	White River Junction	VT	Medium
3	19	436	VA Montana HCS (Ft. Harrison, Miles City)	Fort Harrison	MT	Integrated Medium
4	23	437	Fargo VAMC	Fargo	ND	Small
5	23	438	Royal C. Johnson Veterans Sioux Falls Memorial MC (Sioux Falls)	Sioux Falls	SD	Small
6	19	442	Cheyenne VA Medical	Cheyenne	WY	Medium
7	21	459	VA Pacific Islands HCS (Honolulu)	Honolulu	HI	Medium
8	4	460	Wilmington VAMC	Wilmington	DE	Large
9	20	463	Alaska VA HCS and Regional Office (Anchorage)	Anchorage	AL	Medium
10	18	501	New Mexico HCS (Albuquerque)	Albuquerque	NM	Large
11	16	502	Alexandria VAMC	Pineville	LA	Medium
12	4	503	Altoona - James E. Van Zandt VAMC	Altoona	PA	Medium
13	18	504	Amarillo HCS	Amarillo	TX	Medium
14	11	506	VA Ann Arbor HCS	Ann Arbor	MI	Large
15	7	508	Atlanta VAMC	Augusta	GA	Large
16	7	509	Charlie Norwood VAMC (Augusta)	Augusta	GA	Large
17	5	512	VA Maryland HCS (Baltimore, Loch Raven, Perry Point)	Baltimore	MD	Integrated Large

18	11	515	Battle Creek VAMC	Battle Creek	MI	Large
19	8	516	Bay Pines VAMC	Bay Pines	FL	Large
20	6	517	Beckley VAMC	Beckley	WV	Small
21	1	518	Edit Nourse Rogers Memorial Veterans Hospital (Bedford)	Bedford	MA	Medium
22	17	519	West Texas VA HCS (Big Spring)	Big Spring	TX	Small
23	16	520	VA Gulf Coast HCS (Biloxi)	Biloxi	MS	Large
24	7	521	Birmingham VAMC	Birmingham	AL	Large
25	1	523	VA Boston HCS- (Boston Brockton, West Roxbury	West Roxbury	MA	Integrated Large
26	3	526	James J. Peters (Bronx)	Bronx	NY	Large
27	2	528	Upstate New York HCS (Buffalo, Batavia, Canandaigua, Syracuse, Bath, Albany)	Buffalo	NY	Integrated Large
28	2	528A5	Canandaigua VAMC	Canandaigua	NY	Integrated Large
29	2	528A6	Bath VAMC	Bath	NY	Integrated Large
30	2	528A7	Syracuse VA Medical Center	Syracuse	NY	Integrated Large
31	2	528A8	Albany VA Medical Center (Samuel S. Stratton)	Albany	NY	Integrated Large
32	4	529	VA Butler Healthcare (Butler)	Butler	PA	Medium
33	20	531	Boise VAMC	Boise	ID	Medium
34	7	534	Ralph H. Johnson VAMC (Charleston)	Charleston	SC	Large
35	12	537	Jesse Brown VAMC (Chicago Westside, Chicago Lakeside)	Chicago	IL	Integrated Large
36	10	538	Chillicothe VAMC	Chillicothe	OH	Medium
37	10	539	Cincinnati VAMC	Cincinnati	OH	Large
38	4	540	Louis A Johnson VAMC	Clarksburg	WV	Medium

			(Clarksburg)			
39	10	541	Louis Stokes VAMC (Cleveland)	Cleveland	OH	Large
40	4	542	Coatesville VAMC	Coatesville	PA	Medium
41	7	544	Wm. Jennings Bryan Dorn VAMC (Columbia)	Columbia	SC	Large
42	8	546	Miami VAMC	Miami	FL	Large
43	8	548	W Palm Beach VAMC	West Palm Beach	FL	Large
44	17	549	North Texas VAMC (Dallas, Bonham)	Dallas	TX	Integrated Large
45	11	550	VA Illiana HCS (Danville)	Danville	IL	Large
46	10	552	Dayton VAMC	Dayton	OH	Large
47	11	553	John D. Dingell VAMC (Allen Park, Detroit)	Detroit	MI	Large
48	019	554	VA East Colorado HCS (Denver, Ft. Lyon)	Denver	CO	Integrated Large
49	12	556	Captain James A. Lovell Federal HCC (North Chicago)	North Chicago	IL	Large
50	7	557	Carl Vinson VAMC (Dublin)	Dublin	GA	Medium
51	6	558	Durham VA Medical Center	Durham	NC	Large
52	3	561	New Jersey HCS-East Orange, Lyons)	East Orange	NJ	Integrated Large
53	4	562	Erie VAMC	Erie	PA	Medium
54	16	564	Veterans HCS of the Ozarks (Fayetteville(	Fayetteville	AR	Large
55	6	565	Fayetteville VA Medical Center	Fayetteville	NC	Large
57	23	568	VA Black Hills HCS (Fort Meade, Hot Springs)	Fort Meade	SD	Integrated Small
58	21	570	VA Central California HCS (Fresno)	Fresno	CA	Large
59	8	573	VA North Florida/South Georgia HCS-(Gainesville, Lake City)	Gainesville	FL	Integrated Large

60	19	575	Grand Junction VAMC	Grand Junction	CO	Small
61	12	578	Edward Hines Jr. VA Hospital (Hines)	Hines	IL	Large
62	16	580	Michael E DeBakey VAMC (Houston)	Houston	TX	Large
63	9	581	Huntington VAMC	Huntington	WV	Medium
64	11	583	Richard L.Roudebush. (Indianapolis)	Indianapolis	IN	Large
65	12	585	Iron Mountain VAMC	Iron Mountain	MI	Small
66	16	586	G. V. (Sonny) Montgomery VAMC (Jackson)	Jackson	MS	Large
67	15	589	VA Heartland - West (Kansas City, Topeka, Leavenworth, Wichita)	Kansas City	MO	Integrated Large
68	15	589A4	Columbia VAMC	Columbia	MO	Integrated Large
69	15	589A5	East Kansas HCS	Topeka/ Leavenworth	KS	Integrated Large
70	15	589A7	Wichita Medical Center	Wichita	KS	Integrated Large
71	6	590	Hampton VAMC	Hampton	VA	Large
72	22	593	VA Southern Nevada HCS (Las Vegas)	Las Vegas	NV	Large
73	4	595	Lebanon VAMC	Lebanon	PA	Large
74	9	596	Lexington VAMC (Leestown, Cooper)	Lexington	KY	Large
75	16	598	Central AR. Veterans HCS (Little Rock)	Little Rock	AR	Large
76	22	600	VA Long Beach HCS	Long Beach	CA	Large
77	9	603	Louisville VAMC	Louisville	KY	Large
78	22	605	Jerry L. Pettis Memorial VAMC (Loma Linda)	Loma Linda	CA	Large
79	12	607	William S. Middleton Memorial Veterans Hospital (Madison)	Madison	WI	Large

80	1	608	Manchester VAMC	Manchester	NH	Medium
81	11	610	VA N. Indiana HCS (Marion, Fort Wayne)	Marion	IN	Integrated Large
82	21	612	VA N. California HCS (Mather)	Mather	CA	Integrated Large
83	5	613	Martinsburg VAMC	Martinsburg	WV	Medium
84	9	614	Memphis VAMC	Memphis	TN	Large
85	23	618	Minneapolis VAMC	Minneapolis	MN	Large
86	7	619	VA Hudson Valley HCS (Tuskegee, Montgomery)	Montgomery	AL	Integrated Large
87	3	620	VA Hudson Valley HCS-NY (Montrose, Castle)	Montrose	NY	Integrated Medium
88	9	621	James H. Quillen VAMC (Mountain Home)	Mountain Home	TN	Large
89	16	623	Jack C. Montgomery VAMC (Muskogee)	Muskogee	OK	Large
90	9	626	VA Tennessee Valley HCS (Nashville, Murfreesboro)	Nashville	TN	Integrated Large
91	16	629	Southeast Louisiana Veterans HCS (New Orleans)	New Orleans	LA	Large
92	3	630	New York Harbor HCS- (Brooklyn, Manhattan)	New York	NY	Integrated Large
93	1	631	Northampton VAMC	Leeds	MA	Small
94	3	632	Northport VAMC	Northport	NY	Large
95	16	635	Oklahoma City VAMC	Oklahoma City	OK	Large
96	23	636	VA Nebraska Western Iowa HCS (Omaha, Lincoln, Grand Island of NE, Des Moines, Knoxville, Iowa City of IA) AKA VA Central Plains HCS	Omaha	NE	Integrated Large
97	23	636A6	VA Central Iowa HCS (Des Moines)	Des Moines	IA	Medium
98	23	636A8	Iowa Cite VA HCS	Iowa City	IA	Medium

99	6	637	Asheville VA Medical Center	Asheville	NC	Large
100	21	640	VA Palo Alto HCS (Palo Alto, Livermore)	Palo Alto	CA	Integrated Large
101	4	642	Philadelphia VAMC	Philadelphia	PA	Large
102	18	644	Phoenix VA HCS	Phoenix	AZ	Large
103	4	646	VA Pittsburgh HCS-(Pittsburg Univ Dr, H.J.Heinz Campus)	Pittsburgh	PA	Integrated Large
104	20	648	Portland VAMC	Portland	OR	Large
105	18	649	Northern Arizona VA HCS (Prescott)	Prescott	AZ	Medium
106	1	650	Providence VAMC	Providence	RI	Large
107	6	652	Hunter Holmes McGuire VAMC (Richmond)	Richmond	VA	Large
108	20	653	VA Roseburg HCS	Roseburg	OR	Medium
109	21	654	VA Sierra Nevada HCS (Reno)	Reno	NV	Large
110	11	655	Aleda E. Lutz VAMC (Saginaw)	Saginaw	MI	Medium
111	23	656	St Cloud VAMC	St. Cloud	MN	Small
112	15	657	VA Heartland – East (St Louis, Popular Bluff, Marion)	St. Louis	MO	Integrated Large
113	15	657A4	Popular Bluff Medical Center	Popular Bluff	IL	Integrated Large
114	15	657A5	Marion Medical Center	Marion	MO	Integrated Large
115	6	658	Salem VAMC	Salem	VA	Large
116	6	659	W.G. (Bill) Hefner VAMC (Salisbury)	Salisbury	NC	Large
117	19	660	VA Salt Lake City HCS	Salt Lake City	UT	Large
118	21	662	San Francisco VAMC	San Francisco	CA	Large
119	20	663	VA Pugett Sound (Seattle,	Seattle	WA	Integrated

			Tacoma)			Large
120	22	664	VA San Diego HCS	San Diego	CA	Large
121	19	666	Sheridan VAMC	Sheridan	WY	Small
122	16	667	Overton Brooks VAMC (Shreveport)	Shreveport	LA	Large
123	20	668	Mann-Grandstaff VAMC (Spokane)	Spokane	WA	Medium
124	17	671	VA South Texas VAMC (San Antonio, Kerrville)	San Antonio	TX	Integrated Large
125	8	672	VA Caribbean HCS (San Juan)	San Juan	PR	Large
126	8	673	James A Harley Veteran's' Hospital (Tampa)	Tampa	FL	Large
127	17	674	Central Texas Veterans HCS (Temple, Waco)	Temple	TX	Integrated Large
128	8	675	Orlando VAMC	Orlando	FL	Large
129	12	676	Tomah VAMC	Tomah	WI	Medium
130	18	678	Southern Arizona VA HCS (Tucson)	Tucson	AZ	Large
131	7	679	Tuscaloosa VAMC	Tuscaloosa	AL	Medium
132	20	687	Johnathon M. Wainwright Memorial VAMC (Walla Walla)	Walla Walla	WA	Small
133	5	688	Washington DC VAMC	Washington	DC	Large
134	22	691	VA Greater Los Angeles HCS (Los Angeles, West Los Angeles)	West Los Angeles	CA	Integrated Large
135	20	692	VA Southern Oregon Rehabilitation Ctr & Clinics (White City)	White City	OR	Small
136	1	689	VA Connecticut Health Care System (West Haven, Newington)	West Haven	CT	Integrated Large
137	4	693	Wilkes Barre VAMC	Wilkes-Barre	PA	Large
138	12	695	Clement J. Zablocki VAMC (Milwaukee)	Milwaukee	WI	Large

139	17	740	VA Texas Valley Coastal Bend HCS	Harlingen	TX	Small
140	17	756	El Paso VA HCS	El Paso	TX	Medium
141	10	757	Chalmers P. Wylie VA Ambulatory Care Center (Columbus)	Columbus	OH	Large
142	21	358	Manila Outpatient Clinic (Philippines)		PI	Small

ATTACHMENT B: INTEGRATION CONTROL REGISTRATIONS

The following tables list all the Non-Vista Interfaces and all Integration Control Registrations (ICRs) for which the Fee Basis Claims System is a subscriber. Note that the VA FileMan and Kernel ICRs (numbers 10000 and higher) are supported for use by all Vista applications.

Non-VistA Interfaces

Interface Number	Interface
HCP0001	Eligibility and Enrollment*
HCP0002	Hospital Notification*
HCP003	Referral and Authorization System
PIT001	AITC Drop Zone
RTS001	HAC National MSSQL

*Does not include VistA IFCAP bi-directional interface or alteration to any existing FBCS payment methodology.

ICR Number	ICR Name
287	DBIA287 ($$HDR^FBAAUTL3())
315	DBIA315-A (EN1^PRCS58)
767	DBIA268-C (Access to the DG SECURITY LOG file)
831	DBIA315-B (PRCS58CC)
832	DBIA315-C (PRCSUT31)
1074	VATRAN
1995	CPT Code APIs
1996	CPT/HCPCS Modifier APIs
1997	CPT Utility APIs
2051	Database Server API: Lookup Utilities
2052	Database Server API: Data Dictionary Utilities
2053	Data Base Server API: Editing Utilities
2055	Data Base Server API: Misc. Data Libaray Functions
2056	Data Base Server API: Data Retriever Utilities
2071	CODE INDEX (FPDS)
2171	DBIA2171 (PARENT^XUAF4)
2689	OE/RR references to ALERT file
2716	DG MST STATUS API'S
2834	Calls to TIUSRVLO
2848	GETALL API CALL ($$GETALL^SCAPMCA(DFN))
3771	XUDHGUI
3990	ICD Code APIs
4052	DRG Code APIs
4419	DBIA4419 ($$INSUR^IBBAPI)

4436	DBIA4436 ($$CREATE^DGPTFEE)
4807	API FOR RATED DISABILITIES
5080	5080 - FBAACCB0 for FBCS (DSS)
5081	5081 - FBAACCB2 for FBCS (DSS)
5082	5082 - FBAACO For FBCS (DSS)
5083	5083 - FBAADD for FBCS (DSS)
5084	5084 - FBAADV for FBCS (DSS)
5085	5085 - FBAAFA for FBCS (DSS)
5086	5086 - FBAAFR for FBCS (DSS)
5087	5087 - FBAAFS for FBCS (DSS)
5088	5088 - FBAARB for FBCS (DSS)
5089	5089- FBAARR for FBCS (DSS)
5090	5090 - FBAAUTL for FBCS (DSS)
5091	5091 - FBAAUTL4 for FBCS (DSS)
5092	5092 - FBAAUTL5 for FBCS (DSS)
5093	5093 - FBAAV01 for FBCS(DSS)
5094	5094 - FBAAV6 for FBCS (DSS)
5095	5095 - FBAAVR0 for FBCS (DSS)
5096	5096 - FBCHFA for FBCS (DSS)
5097	5097 - FBCHREQ2 for FBCS (DSS)
5098	5098 - FBCSV1 for FBCS (DSS)
5099	5099 - FBUCUTL for FBCS(DSS)
5100	5100 - FBUCUTL2 for FBCS (DSS)
5104	FBCS File #162.4 R/W/D
5105	5105 - FBAACCB1 for FBCS (DSS)
5106	5106 - FBAAUTL2 for FBCS (DSS)
5107	FBCS FILE 162 R/W/D
5108	FBAAV1 for FBCS (DSS)
5109	FBAAV3 for FBCS (DSS)
5110	FBAAV4 for FBCS (DSS)
5111	FBAAV5 for FBCS (DSS)
5112	FBAASCB for FBCS (DSS)
5113	FBNHEXP for FBCS (DSS)
5114	FBMRASVR for FBCS (DSS)
5115	FBPAY2 for FBCS (DSS)
5116	FBPAY21 for FBCS (DSS)
5117	FBPAY67 for FBCS (DSS)
5118	FBRXFA for FBCS (DSS)
5119	FBRXFR for FBCS (DSS)
5120	FBUTL2 for FBCS (DSS)
5211	FBUCLET for FBCS (DSS)
5212	FBCHFR for FBCS (DSS)
5216	FBAAC04 for FBCS (DSS)
5217	FBAAV2 for FBCS (DSS)
5272	FBCS FILE 161 R/W/D
5273	FBCS FILE #161.7 R/W/D
5274	FBCS FILE 442
5275	FBCS ACCESS TO FILE #161.4 R/O
5276	FBCS File #161.6 Read only
5277	FBCS ACCESS TO FILE #162.5
5278	FBCS File #161.2 Read only
5300	FBCS FILE 424
5301	FBCS FILE 420

5327	FBCS call to FBAAUTL1
5328	FBCS Access to FBCH78
5329	FBCS Access to FBCHACT0
5330	FBCS ACCESS TO PRCSUT
5336	FBCS ACCESS TO GLOBAL PRC(411
5379	FBCS ACCESS TO DGENA
5392	FBCS ACCESS TO FBCHDI
5397	FBCS File #162.7 Read only
5398	FBCS File #161.25 R/W
5400	FBCS File #161.27 Read only
5409	FBCS File #162.1 Read only
5410	FBCS File #162.2 R/W/D
5441	FBCS Access to FBUCUTL5 routine
5442	FBCS Access to FBNPILK
5443	FBCS Access to FBAACO3
5444	FBCS access to FBAASCB0
5524	CHANGE PACKAGE NAME AND DESCRIPTIONS
5573	User OK as Certifier for a 1358?
10000	Classic FileMan API: Date/Time Manipulation
10003	Classic FileMan API: Date/Time Input & Conversion
10005	Classic FileMan API: Required Variables
10008	Classic FileMan API: Entry Display For Lookups
10009	Classic FileMan API: Adding New Entries & YES/NO Prompt
10011	Classic FileMan API: Word Processing
10013	Classic FileMan API: Entry Deletion & File Reindexing
10018	Classic FileMan API: Edit Data
10026	Classic FileMan API: Reader
10060	NEW PERSON FILE
10061	VADPT
10063	%ZTLOAD
10076	XUSEC GLOBAL
10089	%ZISC
10103	XLFDT
10104	XLFSTR